On the post-quantum security of classical authenticated encryption schemes

Nathalie Lang, Stefan Lucks

Motivation

Encryption, message authentication and authenticated encryption

Authenticated Encryption is the combination of not learning what we are sending (*encryption*) and not learning anything about the context (*authentication* → Message Authentication Codes (MACs)).

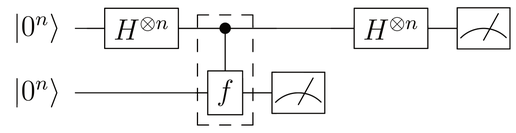
Classical bits vs. qubits

- Classical message (3 bit): 110
- Message(s) in superposition (3 qubit):

$$\alpha_0 |000\rangle + \alpha_1 |001\rangle + \ldots + \alpha_7 |111\rangle$$
$$|\alpha_0|^2 + |\alpha_0|^1 + \ldots + |\alpha_7|^2 = 1$$

Main question: How secure is the authenticated encryption used today once there will be quantum computers?

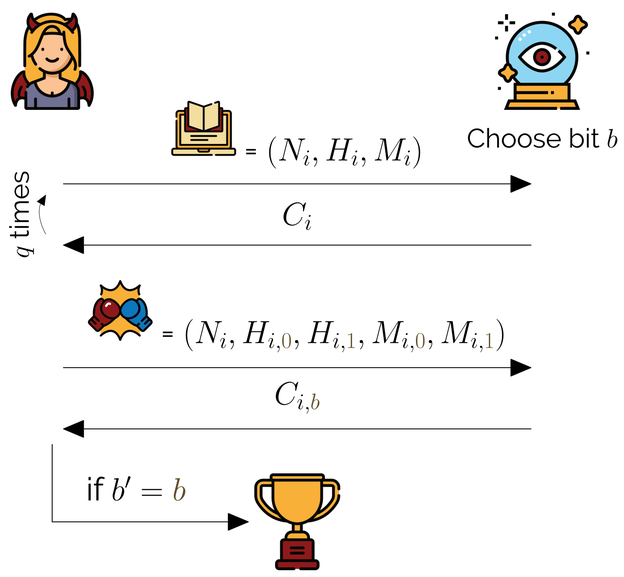
Simon's algorithm



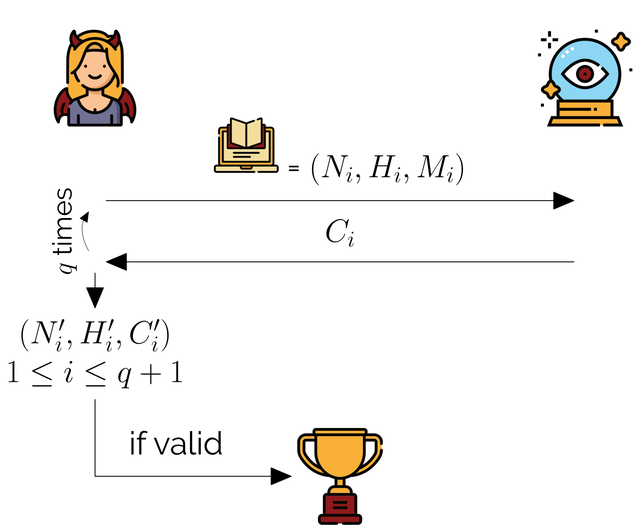
Simon's algorithm uses a quantum computer to find a *hidden shift* ($f(x) = f(x \oplus s) \rightarrow$ hidden shift = s). While a classical computer would need at least $2^{n/2}$ queries, a quantum computer (like the one on the right-hand side) can solve this with at most n queries.

Attacks

Generic security games



The generic IND-CPA game for privacy



The generic PO game for authenticity

Quantum attacks

- In a *Q1* setting, the defender uses a classical computer while the adversary uses a quantum computer.
  - Security against Q1 adversaries is signalized by the number *1* (e.g. IND-1CPA).
- In a *Q2* setting, both use quantum computers.
  - Security against Q2 adversaries is denoted by *q* (e.g. qPO).
- When talking about security against classical adversaries, this is denoted by the letter *c* (e.g. cPO).

Results

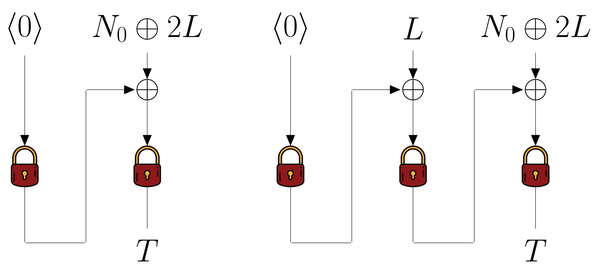
Insecure modes

Mode	Exemplary usage
SIV	Cloud Encryption
GCM	HTTPS
EAX	Successor of CCM used for IOT

Secure Schemes

- Nonce-prefix-MACs (MACs with a number used once as a message prefix)
- Nonce-based key derivation

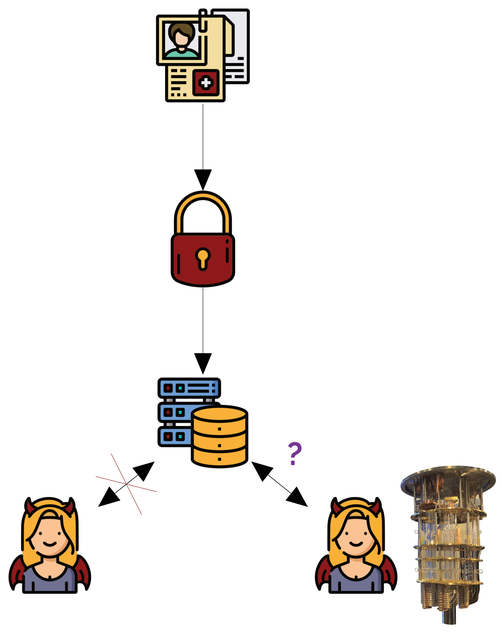
Example: Nonce colision for EAX



- [1] showed how to use Simon's algorithm to recover $L = Enc(0)$.
- Choose a number used once (*nonce*) $N_0 = L \oplus 2L$ of length n and another nonce $N_1 = (L||N_0)$ of length $2n$.
- For both nonces, the authentication tag T will be equal.

Outlook

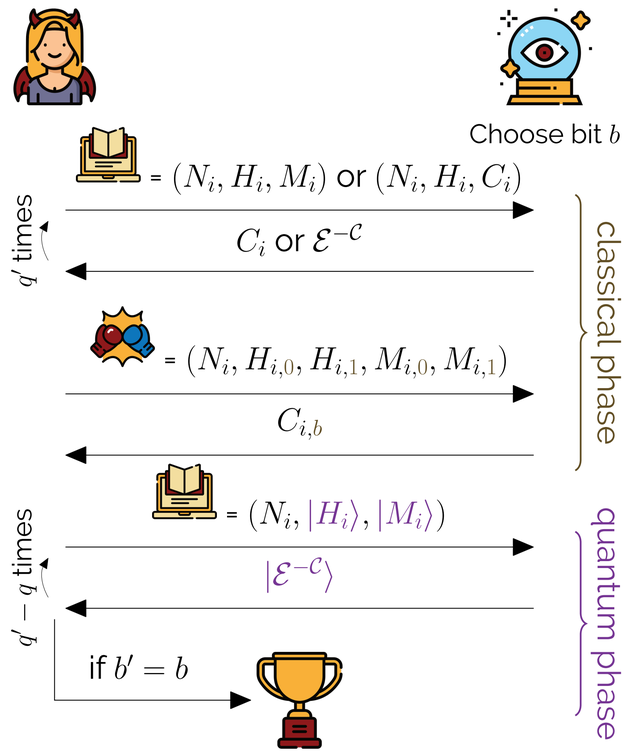
Example: Medical data



Would sensitive data encrypted according to today's standards still be secure if we grant access of quantum computers?

- Assume we are using an IND-1CPA secure AE scheme and suddenly Q2 queries are possible.
- Will we be able to continue using that AE scheme?
- The intention is that it will remain secure under some uncritical assumptions as long as it will be used only in the Q1 model.

We are currently working on proving this claim by introducing the new notion of *Legacy-qCCA*.



The Legacy-qCCA game

Bauhaus-Universität Weimar

References

[1] Marc Kaplan et al. "Breaking Symmetric Cryptosystems Using Quantum Period Finding". *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9815. Lecture Notes in Computer Science. Springer, 2016, pp. 207–237. DOI: 10.1007/978-3-662-53008-5_8. URL: https://doi.org/10.1007/978-3-662-53008-5%5C_8.

Icons used from resources from Flaticon.com
"50 qbit quantum computer" by epgoldator is licensed under CC BY 2.0.